ASA: входящий доступ к сбоям адресов NAT после обновления к 8.4 (3)

Содержание

Введение

Этот документ предоставляет сведения об адресах NAT, которые отказывают после обновления Устройства адаптивной защиты (ASA) к версии 8.4 (3). Этот документ также предоставляет разрешение этой проблеме.

Предварительные условия

Требования

Читатели данного документа должны обладать знаниями по следующим темам.

- Основное понимание концепции адресов Протокол разрешения (ARP) и прокси - протокол преобразования адресов

Используемые компоненты

Сведения в документе приведены на основе данных версий аппаратного и программного обеспечения.

- Любое многофункциональное устройство защиты Cisco ASA серии 5500
- Версия 8.4 (3) Устройства адаптивной безопасности или позже

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips

Conventions.

Признаки

Начиная с версии ASA 8.4 (3) ASA не отвечает на запросы ARP, полученные на интерфейсе для IP-адресов, которые не являются частью IP-подсети того интерфейса. Перед версией 8.4 (3) ASA ответил бы на запросы ARP, которые не были в IP-подсети интерфейса ASA.

Это изменение может сразу проявить себя после обновления ASA к версии 8.4 (3). В некоторых случаях интернет-пользователи не могут соединиться с глобальным адресом преобразованного сервера через ASA.

Это сообщение отображено, если с этой ситуацией встречаются, и 'debug arp' включен на CLI ASA:

```
arp-in: Arp packet received from 192.168.10.1 which is in different subnet
than the connected interface 192.168.11.1/255.255.255.0
```

Основная причина этой проблемы не является дефектом. Посмотрите информацию ниже для узнавания больше о потенциальных причинах и решениях проблемы.

Условия / Среда

Для обнаружения с этой ситуацией ASA должен получить запрос ARP для IP-адреса, который совпадает с глобальным адресом в настроенном преобразовании NAT. Глобальный IP-адрес должен находиться в IP-подсети, которая отличается от IP-подсети, настроенной на интерфейсе ASA.

Причина / Описание проблемы

Для понимания полных ограничений этой проблемы важно получить полное понимание того, как эта проблема может появиться и лучший способ смягчить проблему.

Это некоторые экземпляры, где можно встретиться с этой ситуацией:

Устройству восходящего потока данных настроили IP-маршруты без IP - адреса следующего прыжка

Это - вероятно, наиболее распространенная причина этой ситуации. Это происходит из-за конфигурации неоптимального устройства восходящего потока данных. Это предпочтено для настройки IP-маршрутов, таким образом, что следующим переходом IP-маршрута является IP-адрес в той же подсети как адрес того интерфейса:

```
ip route 10.1.2.0 255.255.255.0 192.168.1.2
```

Однако иногда администраторы сети настраивают интерфейс вместо IP-адреса как следующий переход:

```
ip route 10.1.2.0 255.255.255.0 FastEthernet0/1
```

Это заставляет маршрутизатор направлять трафик, предназначенный к 10.1.2.0/24 сети к интерфейсу FastEthernet0/1 и передавать запрос ARP за IP - адресом назначения в пакете IP. Предполагается, что некоторое устройство ответит на запрос ARP, и маршрутизатор

тогда передает пакет к MAC-адресу, который был решен из-за процесса ARP. Преимущества данного типа конфигурации - то, что очень легко настроить и администрировать. Администратор не должен явно настраивать IP-адрес следующего перехода для маршрута, и они предполагают, что смежному устройству включат Proxy-arp и ответит на запрос ARP, если это будет способно к маршрутизации пакетов к IP - адресу назначения.

Однако существуют серьезные проблемы с этим типом конфигурации IP-маршрута:

- Путем передачи запроса ARP для определения следующего перехода для IP - трафика маршрутизатор представлен проблемам, вызванным другими устройствами, которые могли бы неправильно ответить на тот запрос ARP. Результатом является трафик, может быть помещен в черный список, когда передается неправильному устройству.
- Маршрут заставит устройство передавать запрос ARP за каждым уникальным адресом назначения (DA) в пакетах, которые совпадают с маршрутом. Это может вызвать большое количество трафика ARP на подсети и негативно влиять на производительность, а также область памяти, требуемую держаться потенциально большое количество Записей ARP.
- Поскольку пространство таблицы ARP является связанным ресурсом памяти, избыточное число записей может негативно повлиять на производительность и устойчивость маршрутизатора.

Поэтому оптимальный метод должен настроить все маршруты с адресами следующего узла явного IP и не маршруты использования, которые имеют имя интерфейса отдельно для определения исходящего интерфейса. Если интерфейс необходим для связи маршрута с исходящим интерфейсом для аварийного переключения, введите и имя исходящего интерфейса и следующий переход в статическом маршруте.

Учитывая административные результаты для некоторых Клиентов Cisco, Запрос на расширение был открыт для создания нового безопасного поведения конфигурируемым: Идентификатор ошибки Cisco CSCty95468 (только зарегистрированные клиенты) (ENH: Команда Add для Разрешения Записей кэша ARP от Несвязанных подсетей).

Несогласованные маски подсети IP на смежных устройствах

Несогласованные маски подсети IP, настроенные на интерфейсе ASA и интерфейсе смежного устройства, могут вызвать аналогичную ситуацию. Если смежное устройство имело маску подсети, которая была суперсетью (255.255.240.0) из интерфейсной маски подсети IP ASA (255.255.255.0), смежное устройство будет ARP для IP-адресов, которые не находятся в IP-подсети интерфейса ASA. Гарантируйте, что маски подсети корректны.

Результаты прозрачного режима

Другой побочный эффект этого изменения является неспособностью изучить MAC-адреса из неподключенных напрямую подсетей в Прозрачном режиме. Это влияет на связь в этих сценариях:

- Прозрачному ASA не настроили управление IP-адресами, или конфигурация является неправильной.
- Прозрачный ASA использует вторичные подсети на том же сегменте.

Нет никакого обходного пути для этой проблемы в Прозрачном режиме кроме перехода на более ранние версии. Однако этот Запрос на расширение был открыт, чтобы заставить ASA

взаимодействовать со вторичными подсетями в Прозрачном режиме: Идентификатор ошибки Cisco CSCty49855 (только зарегистрированные клиенты) (ENH: Напрямую подключенные узлы Non Поддержки в Механизме обнаружения MAC).

Разрешение

Решение этой проблемы (в случае, что рассматриваемый IP-адрес не находится в той же подсети уровня 3 как интерфейсный IP ASA) состоит в том, чтобы делать изменения необходимыми, чтобы гарантировать, что устройства, смежные с ASA, направляют трафик непосредственно к IP-адресу интерфейса ASA как устройство на следующем узле, вместо того, чтобы полагаться на устройство к Proxy-arp от имени IP-адреса.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация